UNIFORM SAFEGUARDS FOR PROTECTION OF "CRITICAL SYSTEMS" PROCESSING INTELLIGENCE INFORMATION

December 1984

* * *

Supplement to:
"Security Policy on Intelligence Information in Automated Systems and Networks"
DCID 1/16
dated
4 January 1983

25X1

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

FOREWORD

The Deputy Director of Central Intelligence (DDCI) directed that security SAFEGUARDS be developed to reduce the vulnerabilities associated with processing information derived from sensitive methods and sources in "critical" automated systems and networks. These "critical" systems were identified by the senior members of the intelligence community and uniform assessments of the security of these systems were made using an early draft of these SAFEGUARDS. These SAFEGUARDS identify security requirements which, when satisfied, will significantly reduce the vulnerabilities identified in the assessments of the critical systems. These SAFEGUARD requirements are intended as a transitional step for the Intelligence Community to reduce security risks that are inherent in existing critical systems. The Intelligence Community will use the trusted security products and services of the DoD Computer Security Center as soon as such products and services are developed and are available to be incorporated into the Community's inventory of automated systems. These SAFEGUARDS reflect DCI requirements for reducing near term risks until trusted systems are available and therefore are intended to complement the DoD Computer Security Evaluation Criteria. The SAFEGUARDS are mandatory for all thirteen critical systems and voluntary for all other systems processing information derived from sensitive methods and sources. (U)

Table of Contents

* * * * * * *

I. INTRODUCTION

In May 1983 the Deputy Director of Central Intelligence (DDCI) directed the formulation of Community-coordinated minimum acceptable computer security SAFEGUARDS and standards. These would then be applied to any Community computer networks that might be developed, and would be applied to all computer systems processing and/or storing intelligence information derived from sensitive sources and methods. The DDCI's letter of direction suggested that the DoD Computer Security Evaluation Center's criteria for computer security should be considered as a starting point for development of such minimum SAFEGUARDS. (S)

Approach for Developing Uniform SAFEGUARDS for "Critical Systems"

In response to this DDCI tasking, both short-term (less than 2 years) SAFEGUARDS and long-term (5 to 7 years) standards making approaches were proposed. The longer term approach is to develop broad ranging applicable security standards for the large number of automated systems processing information derived from sensitive intelligence methods and sources. This is to be accomplished through existing organizations such as the Director of Central Intelligence's (DCI) Computer Security Subcommittee. (S)

The short-term approach is to identify a set of uniform security SAFEGUARDS for automated intelligence systems designated as "critical systems." The short-term approach recommended that the uniform computer security SAFEGUARDS developed for these "critical systems" be promulgated by the DDCI. Compliance with these uniform computer security SAFEGUARDS is mandatory for the "critical systems" and voluntary for all other automated systems processing information derived from sensitive intelligence methods and sources until some future time period. The degree of compliance of each "critical system" to each of the applicable uniform SAFEGUARDS identified in this document is specified in the accreditation process for each "critical system." It is estimated that compliance with all applicable uniform SAFEGUARDS in this document is achievable for the "critical systems" within the funding levels identified in the National Foreign Intelligence Program (NFIP) and budget for this purpose. (S)

25X1

25X1

Selection of "Critical Systems"

The "critical systems" to which these uniform security SAFEGUARDS apply were selected by the senior officials in the National Security Community who own and operate this type system. Such systems were designated as critical because of the sensitivity of the data processed and/or the effect that loss of the system or loss of data would have on the Community if the systems were compromised. (S)

Purpose of Field Coordination and Cost Estimates

The "critical systems" processing sensitive intelligence information include large-scale, newly installed automated systems as well as older, single-function systems located throughout the world. Such a wide variety of "critical systems" made it mandatory to coordinate with the field elements that operate these "critical systems" to assess the impact on operations and cost of implementing these SAFEGUARDS before the DDCI issues guidelines regarding their application. Such field assessments have been conducted and the resource estimates have been developed. These field coordinations included cost estimates for the implementation of SAFEGUARDS that are not now available in the "critical systems." These cost estimates and field coordinations were performed to ensure that the set of SAFEGUARDS are achievable and can be implemented, identified, and enforced by appropriate accreditation authorities. (S)

Applicability

This document, which is promulgated as a supplement to DCID 1/16 dated 4 January 1983, identifies uniform security requirements in terms of safeguards to be implemented in automated systems and networks processing information derived from sensitive intelligence methods and sources. (S)

Accreditation

The NFIB member responsible for each "critical system" will approve the data processing requirement and specify the mode of operation for each "critical system." The approval authority for accrediting the "critical system" in the dedicated, system high and compartmented modes of operation is the responsible NFIB member. The approval authority for accrediting any system in the multilevel mode of operation is the DCI (see para 1, Section VII). The NFIB member's accreditation approval authority for "critical systems" and for all other systems operating in the compartmented mode will not be delegated. (C)

II. OBJECTIVE AND GUIDELINES

In order to implement the security policies set forth in Executive Orders 12333 and 12356 and Director of Central Intelligence Directives (DCIDs) 1/17 and 1/16 and in concert with NSDD 145 which was signed by the President on 17 September 1984, this supplement to DCID 1/16 has been developed. It specifies that computer systems processing and/or storing intelligence information derived from sensitive intelligence sources and methods will be provided with controls over the capability of users to cause processing functions to occur within a computer system for system high, compartmented, and multilevel secure modes of operation. In addition, all these modes of operation will continue to rely on environmental and administrative controls for protection. The term "users" as applied throughout this supplement is defined as:

> Users are defined as individuals and/or processes operating on their behalf (e.g., people, programs, processors, networks). This definition of users differs from the DCID 1/16 use of the term. Although not defined by DCID 1/16, the intent of the existing DCID 1/16 document clearly conveys the meaning of user to be an individual. Current technology and the growth in capabilities support the extension of the meaning to include processes operating on behalf of individuals. (U)

The following guidelines shall be used in order to comply with these directives:

25X1

Integration. System control will be effected through the integration of system-specific security features with other environmental and administrative security activities of the host agency(ies) or department(s) (e.g., physical, personnel, communications, emanations, and administrative security). Thus the security of a computer system will incorporate automated security features in addition to environmental and administrative features. (U)

User Identification. Users (see Chapter II, para 1a) will be uniquely identified and their identity will be authenticated by the automated control within the system. (U)

Terminal Identification. The system will provide an automated capability to identify user terminals and other user-employed peripheral devices before allowing them to be used for accessing system resources. (U)

Access Control. Systems will provide access to information or perform functions only as formally authorized for identified users. (U)

Control Labels. All functions or information requiring security protection will have control labels. Labels will be associated with intelligence information output. (U)

Detection. The system will provide functions to detect user actions which are specifically described in the system security policy. (U)

Individual Accountability. Systems processing intelligence information will provide automated audit functions to trace actions of users such that access to specific intelligence information can be reconstructed to provide for a periodic review of individual access or in the event of a deliberate or inadvertent disclosure. For automated message handling systems the automated functions will include provisions for determining who accessed each message. (U)

Auditing. Systems will be able to record the use of security authorized functions and information accesses in order to support detection and accountability. (U)

Security Functions Protection. The security control, parameters, and features (e.g., security control modules, password files, and encryption) for a system will be continuously protected commensurate with the requirements for the protection of the highest level and most restrictive category of classified information processed by the system. (U)

Individual Security Responsibilities. All users of the system will be briefed on the need for exercising sound security practices in protecting the intelligence information processed and/or stored in the system, including input and output. Users will be informed of the security mode in which the system is operating, the types of intelligence information the user is permitted to process and/or store, and that the receipt of any information not specifically requested will be reported immediately to the information system security officer (ISSO), or his designee. (U)

Security Testing. Systems will undergo security tests and evaluations to determine that there are no obvious ways to violate the security policy without detection and to determine that the security capabilities function as specified in the documentation. (U)

Administrative Access Approval. Administrative approvals (not requiring substantive briefings) may be used to grant persons physical access to the central computer facility and remote terminal areas when such persons do not require access to the intelligence information processed and/or stored in the system. The personnel security criteria for granting administrative access to such data is the same as that required for access to substantive intelligence materials. (U)

Maintenance. All maintenance people including vendor personnel who maintain systems will be cleared to the highest level of intelligence information processed by the system/network and be approved for access and bound by the nondisclosure procedures that are placed on personnel approved for access to intelligence information processed by the system/network. (U)

System Security Statement/Plan. A system security statement and plan will be prepared and maintained. The document will identify policy to be followed, degree of compliance, and actions to be taken to modify system security features. (U)

Safeguards Provided by Automated Capabilities Versus Environmental and Administrative Safeguards

The total set of recommended SAFEGUARDS, both those for the near term and those designated for implementation with new hardware/operating systems, inescapably require the effective integration of all security disciplines necessary to protect an operational computer system. These include: hardware/firmware/software, physical, personnel, emanations (TEMPEST), communications, and administrative/procedural security. (U)

The SAFEGUARDS proposed for near-term implementation require a tailored mix of automated, environmental, and administrative security measures for effective employment. The specific combination required stems from the inability, over the near term, to replace the hardware and operating system software for the systems concerned, and the consequent necessity to generate an improved technical base upon which to implement the expanded access control, labeling and audit/accountability capabilities set forth in the accompanying SAFEGUARDS. (U)

While the minimum SAFEGUARDS focus largely on the enhancement of the hardware/software facet, they clearly presuppose, and are dependent upon, an adequate level of security in each of the other security disciplines cited and the effective, comprehensive integration of all applicable security disciplines for each system in its own operational environment. (C)

25X1

Next 36 Page(s) In Document Denied

Approved For Release 2009/06/30 : CIA-RDP89B01354R000100170008-5

IX. GLOSSARY

ACCESS. A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

AUTHENTICATION. A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified.

COMPARTMENTED MODE. See Section VI.

"CRITICAL SYSTEM." For this document, a "critical system" is a computer system processing and/or storing intelligence information that has been selected by senior officials in the National Security Community.

DATAGRAM. A datagram is an internet protocol packet; the packet is made up of a header and trailer. For the purpose of this document the datagram is the equivalent "packet" of data as defined by the network being utilized.

DCI. Director of Central Intelligence.

DCID. Director of Central Intelligence Directive.

DDCI. Deputy Director of Central Intelligence.

DEDICATED MODE. See Section IV.

ESCORT. Duly designated personnel who have appropriate clearances and access approvals for the material contained in the ADP system and are sufficiently knowledgeable to understand the security implications and to control the activities and access of the individual being escorted.

ISSO. Information System Security Officer.

INTELLIGENCE INFORMATION. For purposes of this policy statement, intelligence information means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources and methods, that has been classified pursuant to Executive Order 12356 (or successor order). "Foreign intelligence" and "counterintelligence" have meanings assigned them in Executive Order 12333. "Intelligence," as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982.

LOW WATER MARK. Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the nonhierarchical categories.

MULTILEVEL MODE. See Section VII.

NFIB. National Foreign Intelligence Board.

OBJECT. A passive entity that contains or receives information. Access to an object potentially implies access to information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bytes, words, fields processors, video displays, keyboards, and clocks, printers network nodes, etc.

SBI. Special Background Investigation.

SENSITIVE COMPARTMENTED INFORMATION (SCI). All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

SENSITIVITY LABEL. A piece of information that represents the security level of an object and that describes the sensitivity (e.g. classification) of the data in the object.

SESSION. An activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of logoff).

SESSION SECURITY LEVEL. The security level of a session is the low water mark of the security levels of: the user, the terminal, a level specified by the user, and the system from which the session originates.

STORAGE OBJECT. An object that supports both read and write accesses.

SUBJECT. An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

SUBJECT SECURITY LEVEL. A subject's security level is equal to the security level of the objects to which it has either read only or both read and write access. A subject's security level must always be dominated by the session security level.

SYSTEM HIGH MODE. See Section V.

TRUSTED. Employing sufficient integrity measures to allow its use for processing intelligence information involving sensitive sources and methods.

USER. A user is an individual and/or processes operating on his or her behalf.